(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년11월07일
(11) 등록번호 10-0867353
(24) 등록일자 2008년10월31일

(51) Int. Cl.
H04L 9/30 (2006.01) *H04L 9/32* (2006.01)
(21) 출원번호 10-2006-0110270
(22) 출원일자 2006년11월09일
심사청구일자 2006년11월09일
(65) 공개번호 10-2008-0044925
(43) 공개일자 2008년05월22일

(73) 특허권자
인하대학교 산학협력단
인천 남구 용현동 253 인하대학교
(72) 발명자
양대헌
인천 남구 용현4동 인하대학교 하이테크센터 317호
아지즈
인천 남구 용현4동 인하대학교 하이테크센터 307호
맹영재
인천 남구 용현4동 인하대학교 하이테크센터 307호
(74) 대리인
이은철

전체 청구항 수 : 총 4 항 심사관 : 양종필

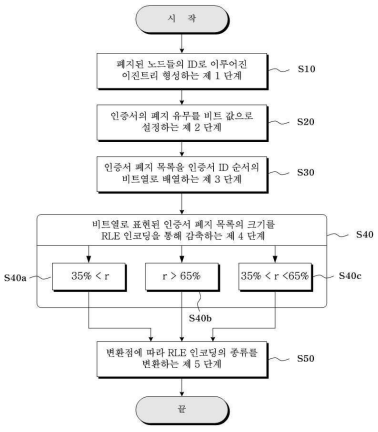
(54) WSN에서의 효율적 통신을 위한 인증서 폐지 목록감축방법

(57) 요 약

본 발명은 WSN에서의 효율적 통신을 위한 인증서 폐지 목록 감축방법에 관한 것으로서, (a) 폐지된 노드들의 ID로 이루어진 이진트리를 형성하는 단계; (b) 인증서의 폐지 유무를 비트 값으로 설정하는 단계; (c) 상기 비트 값을 바탕으로 인증서 폐지 목록을 인증서 ID 순서의 비트열로 배열하는 단계; (d) 비트열로 배열된 인증서 폐지 목록의 크기를 RLE 인코딩을 통해 감축하는 단계; 및 (e) 변환점에 따라 RLE 인코딩의 종류를 변환하는 단계; 를 포함한다.

상기와 같은 본 발명에 따르면, CS 및 BVS 방법을 이용하여 통신 오버헤드를 줄이고, 네트워크상에서 공개키를 관리하는데 필요한 인증서 폐지 목록의 크기를 감축함으로써, 자원이 적게 드는 공개키를 이용한 효율적인 무선 센서 네트워크를 구축할 수 있는 효과가 있다.

대 표 도 - 도1



특허청구의 범위

청구항 1

WSN에서의 효율적 통신을 위한 인증서 폐지 목록 감축방법에 있어서,

(a) 폐지된 노드들의 ID로 이루어진 이진트리를 형성하는 단계;

(b) 인증서의 폐지 유무를 비트 값으로 설정하는 단계;

(c) 상기 비트 값을 바탕으로 인증서 폐지 목록을 인증서 ID 순서의 비트열로 배열하는 단계;

(d) 비트열로 배열된 인증서 폐지 목록의 크기를 RLE 인코딩을 통해 감축하는 단계; 및

(e) 변환점에 따라 RLE 인코딩의 종류를 변환하는 단계; 를 포함하는 WSN에서의 효율적 통신을 위한 인증서 폐지 목록 감축방법.

청구항 2

제 1 항에 있어서,

상기 이진트리의 노드에 속한 인증서가 폐지되었을 경우, 루트에서부터 인증서가 폐지된 노드까지의 경로를, 하나의 인증서 폐지 집합 ID로 설정하는 것을 특징으로 하는 WSN에서의 효율적 통신을 위한 인증서 폐지 목록 감축방법.

청구항 3

제 1 항에 있어서,

상기 (a) 단계의 이진트리에서, 리프노드의 식별자 중, 부모노드로부터 왼쪽은 0, 오른쪽은 1 로 설정하는 것을 특징으로 하는 WSN에서의 효율적 통신을 위한 인증서 폐지 목록 감축방법.

청구항 4

제 1 항에 있어서,

상기 (b) 단계의 초기 비트벡터는, N 개의 인증서 수만큼 '1' 로 설정된 후, 인증서가 폐지될 경우, 해당 인증서 위치의 '1' 앞에 '0' 을 추가하는 것을 특징으로 하는 WSN에서의 효율적 통신을 위한 인증서 폐지 목록 감축방법.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<5> 본 발명은 인증서 폐지 목록 감축방법에 관한 것으로서, 더욱 상세하게는 무선 네트워크상에서 공개키를 관리하는데 필요한 인증서의 폐지 목록의 길이를 줄이기 위한 방법에 관한 것이다.

<6> WSN(Wiress Sensor Network)는 메모리, 연산 통신 등의 자원이 제한된 다량의 센서 노드(Node)로 이루어져 있다. 이러한 센서 노드에서 통신을 위한 연산은 디바이스 내부의 명령어 처리보다 더욱 많은 양의 자원을 필요로 하는데, 실례로 기존의 센서노드 플랫폼의 100미터 링크에서 1Kbit의 전송은 약 3백만 개의 명령어를 필요로 한다. 자원이 제한적인 WSN의 특성에 기인하여 센서노드에서 감지된 데이터를 보증하기 위한 많은 다양한 프로토콜 방법 그리고 오버헤드를 측정하는 접근들은 주로 대칭키 암호로 연구되어 왔다.

<7> 이러한 대칭키 암호는 센서노드에서 공개키 암호에 비해 연산 량이 적으며 상대적으로 적은 통신과 저장 공간을 필요로 하나, 통신하려는 양쪽 모두 반드시 키를 안전하게 교환해야만 하는 문제점이 있었다. 현재, 이러한 문제점을 해소하기 위한 효과적인 해결책으로서, 키 선분배 방법이 연구되고 있다.

<8> 키 선분배 방법은 안전한 통신을 위해 미리 분배된 키 묶음 또는 키의 재료가 센서노드의 메모리에 저장되는 형

식으로서, 그 연결성 및 확장성에 제한이 있었으나, 공개키 암호가 이러한 키 선분배의 문재를 해결한다. 상술한 공개키 암호는 센서노드가 사전절차 없이도 통신할 수 있으며, 손상된 노드의 공개/비밀키가 노출되어도 다른 노드에게 영향을 주지 않는 특징을 갖는다.

<9> 최근의 연구에서 보인 공개키 암호의 효율적인 연산에도 불구하고 WSN에서 공개키 암호를 사용하기에는 이른 감이 있으나, WSN에서 공개키 암호가 사용될 것을 고려하면 공개키를 관리하는 방법이 필요하다.

<10> 한편, 기존의 네트워크에서 전자서명은 키 분배와 인증을 목적으로 사용되었으며, 인증서를 무효화하기 위한 방법으로서 인증서 폐지를 택하게 된다. X.509와 같은 전자서명은 인증서 ID, 공개키(1024 RSA, 320 ECC), 인증서 정보와 이들에 대한 전자서명을 포함한다. 인증서 폐지가 요구됨에 따라 폐지할 인증서에 해당하는 ID의 인증서 폐지 목록(Certificate Revocation List: CRL)을 각 노드에 전달해야 한다. 이에 따른 통신 오버헤드는 기존의 많은 유/무선 네트워크에서는 가능할 수 있으나, 무선 센서 네트워크에서는 이러한 통신 오버헤드는 부담으로 작용한다.

발명이 이루고자 하는 기술적 과제

<11> 본 발명은 상기와 같은 문제점을 해결하기 위해 창안된 것으로서, 네트워크상에서 공개키를 관리하는데 필요한 인증서 폐지 목록의 크기를 감축할 수 있는 방법을 제공함으로써 통신 오버헤드를 줄이는데 그 목적이 있다.

발명의 구성 및 작용

<12> 본 발명은 WSN에서의 효율적 통신을 위한 인증서 폐지 목록 감축방법에 관한 것으로서, (a) 폐지된 노드들의 ID로 이루어진 이진트리를 형성하는 단계; (b) 인증서의 폐지 유무를 비트 값으로 설정하는 단계; (c) 상기 비트 값을 바탕으로 인증서 폐지 목록을 인증서 ID 순서의 비트열로 배열하는 단계; (d) 비트열로 배열된 인증서 폐지 목록의 크기를 RLE 인코딩을 통해 감축하는 단계; 및 (e) 변환점에 따라 RLE 인코딩의 종류를 변환하는 단계; 를 포함한다.

<13> 구체적으로, 상기 이진트리의 노드에 속한 인증서가 폐지되었을 경우, 루트에서부터 인증서가 폐지된 노드까지의 경로를, 하나의 인증서 폐지 집합 ID로 설정하는 것을 특징으로 한다.

<14> 또한, 상기 (a) 단계의 이진트리에서, 리프노드의 식별자 중, 부모노드로부터 왼쪽은 0, 오른쪽은 1 로 설정하는 것을 특징으로 한다.

<15> 그리고, 상기 (b) 단계의 초기 비트벡터는, N 개의 인증서 수만큼 '1' 로 설정된 후, 인증서가 폐지될 경우, 해당 인증서 위치의 '1' 앞에 '0' 을 추가하는 것을 특징으로 한다.

<16> 본 발명의 특징 및 이점들은 첨부도면에 의거한 다음의 상세한 설명으로 더욱 명백해질 것이다. 이에 앞서, 본 명세서 및 청구범위에 사용된 용어나 단어는 발명자가 그 자신의 발명을 가장 최선의 방법으로 설명하기 위해 용어의 개념을 적절하게 정의할 수 있다는 원칙에 입각하여 본 발명의 기술적 사상에 부합하는 의미와 개념으로 해석되어야 할 것이다. 또한, 본 발명에 관련된 공지 기능 및 그 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는, 그 구체적인 설명을 생략하였음에 유의해야 할 것이다.

<17> 이하, 첨부된 도면을 참조하여 본 발명을 상세하게 설명한다.

<18> 본 발명의 일실시예에 따른 WSN에서의 효율적 통신을 위한 인증서 폐지 목록 감축방법에 관해 도 1 내지 도 5를 참조하여 설명하면 다음과 같다. 이하, 본 발명은 Complete Subtree(이하, 'CS') 및 Run-length encoding (이하, 'RLE')를 이용하는 바, 그 이용방법은 하기의 내용을 통해 명확해 질 것이다.

<19> 도 1 은 WSN에서의 효율적 통신을 위한 인증서 폐지 목록 감축방법에 관한 전체 흐름도이며, 도 2 는 CS의 알고리즘을 표현한 일예시도이며, 도 3 은 CS의 완전이진트리를 보여주는 일예시도이며, 도 4 및 도 5 는 RLE 인코딩 종류에 따라 변환된 인코딩 길이를 보여주는 일예시도이다.

<20> 먼저, 폐지된 노드들의 ID로 이루어진 이진트리를 형성하는 단계에 관해 살피면 다음과 같다(S10).

<21> 집합 표현방법을 이용하는 CS(Complete Subtree)는, N:|N| = N개의 리프노드(leaf node)들이 다른 네트워크 노드를 표현하는 완전이진트리(Complete Binary Tree) T를 이용한다. 이때, 루트에서부터 리프노드까지의 경로는 리프노드의 식별자(ID)를 나타내며, 폐지될 노드들의 식별자는 R = V1, V2....Vr : |R| = r 로 표기한다. 상술한 리프노드의 식별자 중, 부모노드로부터 왼쪽은 0, 오른쪽은 1 로 설정한다. Broadcast Encryption의 CS는 키를 각 노드에 할당하는 것에 의의가 있으나, 본 실시예에서는, 임의의 노드를 최소 개수의 집합으로 표현하는

방법에 사용하도록 한다.

<22> 즉, 완전이진트리에서 리프들의 그룹 R⊂T의 CS인 $V_1 \ldots V_t$bT의 집합을 찾음으로써, 노드 $v_{i1} \ldots v$는 i가 $0 < i < t, V_i$j$V_j = \in$ ($i@j$그리고V_1j$V_2 \ldots V_t = R$)일 때, V_i의 자식 노드들을 나타낸다. V_i의 ID는 루트로부터 V_i 까지의 경로를 나타내는 이진 문자열이므로 ID의 길이는 언제나 $\log_2(N)$이하이다. 상기 CS는 CRL ID들의 통신 오버헤드를 줄이는데 바로 적용될 수 있다. 오버헤드가 $r < 5\%$일 때 효율을 보이기 시작하고 오버헤드가 충분히 클 때($r > 20\%$) 상당한 압축 효과를 보인다.

<23> Run-length encoding(이하, 'RLE')는 이진 문자열 P를 인코딩된 스트링 C 로 만드는 데이터 인코딩 알고리즘이다. 그 일예로서, 1RLE-4b는 {1, 01, 001, 0001, 00001, 000001, 0000001, 00000001, 00000000} ² {0, 1, 2, 3, 4, 5, 6, 7, 8}과 같이 P → C로 매치되는데 여기서 각각의 C 는 단일표현 '1' (1RLE-4b에서는 8)을 제외하고 4비트의 코드워드로 인코딩된다. 인코딩 전의 '1' 또는 '0'은 평문의 비트를 표현하며, 1-RLE는 P 에서의 '1'을, 0-RLE는 P 에서의 '0'을 run-length로 표현하는데 사용한다.

<24> 다음으로, 인증서의 폐지 유무를 비트 값으로 설정하는 단계를 살피면 다음과 같다(S20). N 개의 노드를 N 개의 비트로 표현한 비트 벡터에서, i번째 비트가 '0'이라면 폐지되지 않은 인증서를 나타내고, '1' 이라면 폐지된 인증서를 나타낸다. 노드는 이 비트벡터에서 1의 위치를 보고 어느 인증서가 폐지되었는지 알 수 있다. 이와 같이 폐지를 한번만 고려한 BVS를 BVS-S(Static)라고 하며 BVS-S의 길이는 N 비트이다.

<25> 대부분의 시스템에서 한번 인증서가 폐지되면 다른 ID를 가진 인증서가 그것을 대체하는데(같은 ID에 다른 파라미터를 가질 수 도 있다) BVS-S는 폐지를 한번만 고려하여 실제 시스템에서 사용하기에는 다소 무리가 있다.

<26> 따라서, 각 센서마다 폐지 횟수를 고려하여 미리 고정된 공간 바람직하게, '10' 을 만들어 놓고, 폐지될 때마다 한 자리씩 증가시키는 방법을 생각할 수 있지만, 이 방법은 폐지된 인증서의 수가 적을 때는 효율적이지 않다.

<27> 이에 따라, 동적인 폐지를 위한 공간을 미리 할당하는 낭비를 줄이기 위해 BVS-S를 다음과 같이 수정한 BVS-D를 제시한다. 즉, 전술한 바와 같이, 인증서의 폐지 유무를 비트 값으로 설정한 후, 인증서 폐지 목록을 인증서 ID 순서의 비트열로 배열하는 단계를 살피면 다음과 같다(S30).

<28> 초기의 비트벡터는 N 길이만큼 '1'로 설정해 놓고 인증서가 폐지되면 해당 인증서위치의 '1'앞에 '0'을 추가한다. 1bit추가 때마다 한 번의 폐지을 의미하며 i 번째 인증서가 유효한지 여부를 확인하려면 i 번째 블록의 0의 개수(n)를 알면되며, 노드 i 를 위한 인증서는 (n+1) 번째에 위치하게 된다. i 번째 블록은 비트벡터에서 i 번째 '1'과 (i-1) 번째 '1'뒤의 '0'들로 이루어져 있다. 앞서 언급된 BVS-S는 폐지의 횟수에 제한을 두어야 했지만 이 방법은 폐지의 횟수에 제한이 없다.

<29> 원래의 CRL에서는 더 큰 범위의 ID가 10번의 폐지를 가능하게 한다. (Naive-D: 10,000개의 인증서를 표현하기 위해 14비트가 필요하고 각각 최대 10번의 폐지를 고려하여 4비트를 추가한 18비트의 ID를 사용한다)

<30> 제안하는 방법에서 자주 등장하는 것처럼, 같은 비트가 연속해서 나타난다면, 효율적인 압축을 위해 RLE와 같은 인코딩 방법을 사용하기에 적절하다.

<31> 따라서, 상기 S30 단계를 통해 비트열로 배열된 인증서 폐지 목록의 크기를 아래에서 제시하는 RLE 인코딩을 통해 감축하는 단계를 살피면 다음과 같다(S40).

<32> 먼저, 폐지된 인증서의 수(r)가 소정 비율 이하일 경우($r < 35\%$), 1RLE-4b와 1RLE-2b는 CRL을 줄이는데 적절한 효율을 보여주고 원래의 N 비트보다 적은 사이즈를 유지하게 한다(S40a). 또한, 폐지된 인증서의 수(r)가 소정 비율이상일 경우($r > 65\%$), 반대로 인코딩(0RLE-2b, 0RLE-4b)하여, 폐지의 수가 많을수록 압축효율이 떨어져 인코딩 길이가 길어지는 것을 대체한다(S40b). 그리고, 그 외($35\% \mathrm{D} r \mathrm{D} 65\%$)구간에서는 N 비트의 BVS-S를 그대로 사용하여 모든 경우에 N 비트 이하의 길이를 유지한다(S40c).

<33> 마지막으로, 변환점에 따라 RLE 인코딩의 종류를 변환함으로써, RLE 인코딩의 길이를 N 비트 이하로 유지한다

(S50). 도 3 및 도 4 에 도시된 바와 같이, 동적인 인코딩 파라미터의 변환점을 찾기 위해 다양한 $r\%$ 와 파라미터들을 이용하여 변환점을 지정한다.

<34> 이상으로 본 발명의 기술적 사상을 예시하기 위한 바람직한 실시예와 관련하여 설명하고 도시하였지만, 본 발명은 이와 같이 도시되고 설명된 그대로의 구성 및 작용에만 국한되는 것이 아니며, 기술적 사상의 범주를 일탈함이 없이 본 발명에 대해 다수의 변경 및 수정이 가능함을 당업자들은 잘 이해할 수 있을 것이다. 따라서, 그러한 모든 적절한 변경 및 수정과 균등물들도 본 발명의 범위에 속하는 것으로 간주되어야 할 것이다.

발명의 효과

<35> 상기와 같은 본 발명에 따르면, CS 및 BVS 방법을 이용하여 통신 오버헤드를 줄이고, 네트워크상에서 공개키를 관리하는데 필요한 인증서 폐지 목록의 크기를 줄임으로써, 자원이 적게 드는 공개키를 이용한 효율적인 무선 센서 네트워크를 구축할 수 있는 효과가 있다.

도면의 간단한 설명

<1> 도 1 은 본 발명의 일실시예에 따른 WSN에서의 효율적 통신을 위한 인증서 폐지 목록 감축방법에 관한 전체 흐름도.

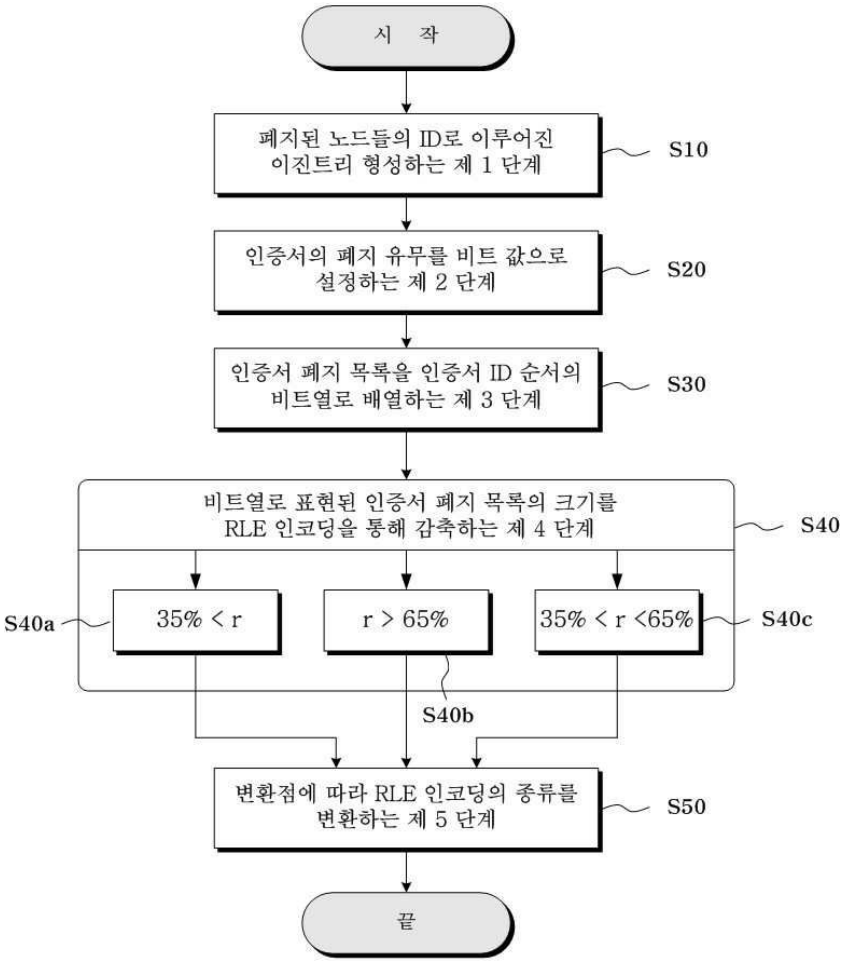
<2> 도 2 는 본 발명의 일실시예에 따른 CS의 알고리즘을 표현한 일예시도.

<3> 도 3 은 본 발명의 일실시예에 따른 CS의 이진트리를 보여주는 일예시도.

<4> 도 4 및 도 5 는 RLE 인코딩 종류에 따라 변환된 인코딩 길이를 보여주는 일예시도.

도면

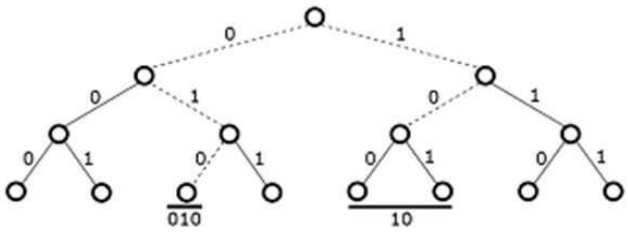
도면1



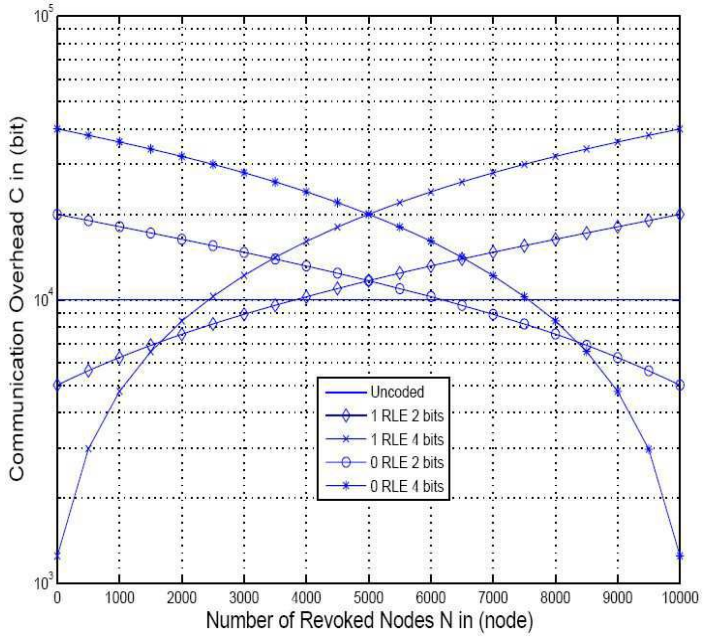
도면2

```
for (i = depth; i > 0; i--) {
    for (j = 0; j < N; j += 2) {
        if (CS[j][i] == 1 && CS[j + 1][i] == 1) {
            CS[j/2][i-1] = 1;
            CS[j][i] = NULL;
            CS[j + 1][i] = NULL;
                                }
            }
    }
```

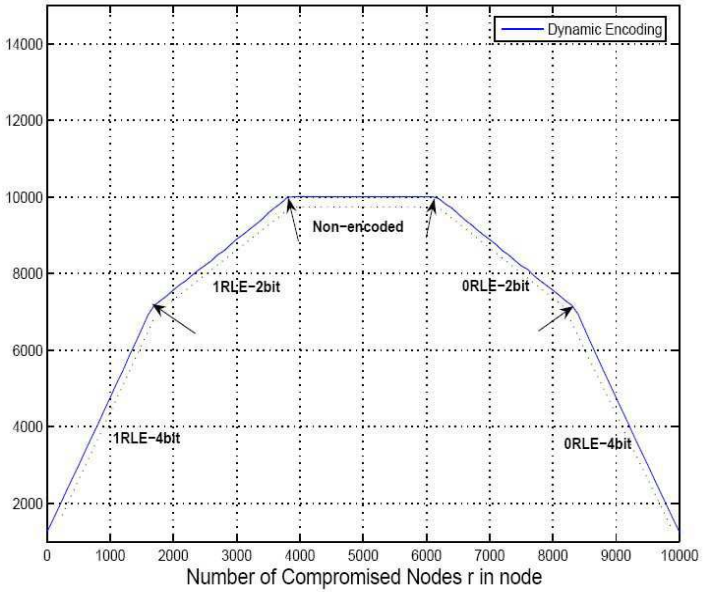
도면3



도면4



도면5


Dynamic Encoding
14000
12000
10000
8000
6000
4000
2000
0
1000
2000
3000
4000
5000
6000
7000
8000
9000
10000
Non-encoded
1RLE-2bit
0RLE-2bit
1RLE-4bit
0RLE-4bit
Number of Compromised Nodes r in node